Amendments to the Claims

This listing of claims supersedes all prior listing of claims.

1. (canceled)

2. (currently amended) A method for encrypting information in a message that can be authenticated, the method comprising:

adding a first authentication block to the information to be encrypted to form a concatenated field;

logically subdividing the concatenated field into predetermined block lengths, including a residual field when the concatenated field is not sized as an even multiple of the predetermined block length;

encrypting the subdivided fields using a first key to form cipher blocks;

designating one of the cipher blocks as a designated cipher block, the other cipher blocks being nondesignated cipher blocks;

subdividing the designated cipher block into a first cipher subblock and a second cipher subblock, such that a combined length of the second cipher subblock and the residual field and a second authentication block is the predetermined block length;

encrypting the second cipher subblock and the residual portion together with the second authentication block using a second key to form a cipher residual block; and

providing at least the first cipher subblock ~~portion~~ of the designated cipher block, the nondesignated cipher blocks and the cipher residual block as the message such that the message can be authenticated by decryption of a valid authentication block of either the first authentication block or the second authentication block.

3. (currently amended) The method of the claim 2, wherein the second authentication block comprises one or more bits and the second cipher subblock ~~portion~~ is less than 128 bits.

4. (previously presented) The method of claim 2, wherein the second authentication block comprises one or more bits forming a null value.

5. (currently amended) A method for encrypting and decrypting information in a message that can be authenticated, the method comprising:

adding a first authentication block to the information to be encrypted to form a concatenated field;

logically subdividing the concatenated field into predetermined block lengths, including a residual field when the concatenated field is not sized as an even multiple of the predetermined block length;

encrypting the subdivided fields using a first key to form cipher blocks;

designating one of the cipher blocks as a designated cipher block, the other cipher blocks being nondesignated cipher blocks;

subdividing the designated cipher block into a first cipher subblock and a second cipher subblock, such that a combined length of the second cipher subblock and the residual field and a second authentication block is the predetermined block length;

encrypting the second cipher subblock and the residual portion together with the second authentication block using a second key to form a cipher residual block; ~~and~~

providing at least the first cipher subblock ~~portion~~ of the designated cipher block, the nondesignated cipher blocks and the cipher residual block as the message such that the message can be authenticated by decryption of a valid authentication block of either the first authentication block or the second authentication block;

decrypting at least the cipher residual block to obtain a representation of the second authentication block;

authenticating the message by comparing the representation of the second authentication block to an expected value for the second authentication block;

decrypting the cipher blocks to obtain at least a representation of the first authentication block; and

further authenticating the message by comparing the representation of the first authentication block to an expected value for the first authentication block.

6. (new) A method for encrypting information in a message that can be authenticated, the method comprising:

adding a first authentication block to the information to be encrypted to form a concatenated field;

logically subdividing the concatenated field to include a residual field;

encrypting the subdivided fields using a first key to form cipher blocks;

designating one of the cipher blocks as a designated cipher block, the other cipher blocks being nondesignated cipher blocks;

subdividing the designated cipher block into a first cipher subblock and a second cipher subblock;

encrypting the second cipher subblock and the residual portion together with a second authentication block using a second key to form a cipher residual block; and

providing at least the first cipher subblock of the designated cipher block, the nondesignated cipher blocks and the cipher residual block as the message such that the message can be authenticated by decryption of a valid authentication block of either the first authentication block or the second authentication block.

7. (new) The method of the claim 6, wherein the second authentication block comprises one or more bits and the second cipher subblock is less than 128 bits.

8. (new) The method of claim 6, wherein the second authentication block comprises one or more bits forming a null value.

9. (new) A method for decrypting information in a message that can be authenticated, the message containing a first cipher block and a second cipher block subdivided from an authentication block combined with information in the message, the second cipher block being combined with a residual field and a second authentication block and being encrypted therewith to form a cipher residual block, the method comprising:

decrypting at least the cipher residual block of the message to obtain a representation of a second authentication block;

authenticating the message by comparing the representation of the second authentication block to an expected value for the second authentication block;

decrypting the first cipher block and the second cipher block to obtain at least a representation of a first authentication block; and

further authenticating the message by comparing the representation of the first authentication block to an expected value for the first authentication block.

10. (new) The method of the claim 9, wherein the second authentication block comprises one or more bits.

11. (new) The method of claim 9, wherein the second authentication block comprises one or more bits forming a null value.